



OSINT + ARCO + PROTECCIÓN DE DATOS

# MAPA-RD: Exposición y Ruta de Cierre

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable.

Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

Felipe de Jesús Miramontes Romero · Reporte RPT-2026-002 · 2026-01-12

Reporte Ejecutivo de Seguridad · Exposición pública · Estrictamente Confidencial

# Índice de Riesgo Digital

Evaluación Cuantitativa de Postura (Estado Global)

---



94

RIESGO MÁXIMO

## Diagnóstico Operativo

**Urgencia Inmediata:** Un IRD de 94 señala un **Máximo riesgo sistémico**. Datos sensibles (financieros/accesos) están expuestos activamente. Se requiere **contención de emergencia** para evitar fraude inminente.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-001

## Banorte: Fuga de Datos Bancarios y PII

95 Máximo

Activo:

Sector Financiero

Tipo:

Identidad Bancaria

Exposición:

Filtración Masiva (2024)

### Ruta de cierre

1. Activar alertas biométricas en banca móvil.
2. Revisar historial crediticio (Buró de Crédito).
3. Solicitar renovación de tarjetas y credenciales.

### Impacto

- Robo de Identidad Bancaria y Fiscal (RFC).
- Ingeniería Social dirigida de alta precisión.
- Riesgo de extorsión o fraude telefónico.

### Descripción del evento

Exposición crítica de datos personales y financieros incluyendo saldos de cuenta, RFC, domicilio físico y números de teléfono. Esta información facilita el robo de identidad y fraude bancario directo.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-002

## Synthient: Credenciales Activas

90 Máximo

Activo:

Identidad Digital

Tipo:

Botnet Logs

Exposición:

Credential Stuffing (2025)

### Ruta de cierre

1. Cambio global de contraseñas de manera inmediata.
2. Uso gestor de contraseñas para evitar reutilización.
3. Habilitar 2FA/MFA en todos los servicios críticos.

### Impacto

- Compromiso automatizado de cuentas en diversos servicios.
- Evasión de controles de seguridad básicos.
- Acceso no autorizado persistente.

### Descripción del evento

El correo y contraseñas asociadas aparecen en listas de amenazas activas de 'Credential Stuffing' (Synthient). Esto indica que los datos están siendo probados activamente contra múltiples servicios.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-003

## 000webhost: Contraseñas en Texto Plano

88 Máximo

Activo:

Hosting Web

Tipo:

Servicio de Infraestructura

Exposición:

Texto Plano (2015)

### Ruta de cierre

1. Abandonar el uso de esa contraseña específica definitivamente.
2. Verificar integridad de sitios web antiguos.
3. Monitorear accesos no reconocidos.

### Impacto

- Acceso inmediato a cuentas con la misma contraseña.
- Rastreo de actividad por dirección IP.
- Compromiso de sitios web alojados.

### Descripción del evento

Filtración de base de datos completa exponiendo contraseñas almacenadas en texto plano, junto con nombres y direcciones IP. Permite acceso directo sin necesidad de descifrado.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-007

## Nitro PDF: Documentos y Claves

82 MÁXIMO

Activo:

Productividad

Tipo:

Software SaaS

Exposición:

Base de Datos (2020)

### Ruta de cierre

1. Revisar documentos almacenados en la nube de Nitro.
2. Cambiar contraseña y desvincular sesiones.

### Impacto

- Espionaje corporativo o personal.
- Acceso a documentos sensibles almacenados.
- Fraude documental.

### Descripción del evento

Compromiso de servicio de gestión documental. Además de credenciales, existe riesgo sobre metadatos de documentos procesados.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-006

## Collection #1: Mega-Brecha

80 MÁXIMO

Activo:

Múltiples Servicios

Tipo:

Agregador de Brechas

Exposición:

Data Dump Masivo (2019)

### Ruta de cierre

1. Higiene digital completa: cambio masivo de claves.
2. Uso estricto de gestor de contraseñas.

### Impacto

- Exposición universal a actores de amenaza.
- Saturación de intentos de login.
- Venta de datos en lotes masivos.

### Descripción del evento

Su correo forma parte de una de las colecciones más grandes de credenciales robadas (773 millones de registros Unique), distribuidas ampliamente en foros de hacking.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-005

## Exploit.In: Listas de Combo

78 CRÍTICO

Activo:

Identidad Digital

Tipo:

Mercado Negro

Exposición:

Agregador de Brechas (2016)

### Ruta de cierre

1. Eliminar cuentas en desuso.
2. Verificar actividad en correos secundarios.

### Impacto

- Alta probabilidad de intentos de acceso automatizados.
- Reutilización de credenciales en servicios bancarios/correo.

### Descripción del evento

Aparición en 'Combo Lists' utilizadas por cibercriminales para ataques de fuerza bruta automatizados contra múltiples plataformas.



# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-004

## Adobe: Compromiso de Credenciales

75 CRÍTICO

Activo:

Cuenta Adobe ID

Tipo:

Software SaaS

Exposición:

Base de Datos (2013)

### Ruta de cierre

1. Actualizar cuenta de Adobe si sigue activa.
2. No utilizar pistas de contraseña que revelen información real.

### Impacto

- Deducción de patrones de contraseñas personales.
- Ataques dirigidos a cuentas creativas/profesionales.
- Spam y phishing dirigido.

### Descripción del evento

Brecha histórica masiva exponiendo usuarios, contraseñas cifradas y, críticamente, las pistas de contraseña (password hints) en texto plano, lo que facilita la deducción de claves.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-008

## 123RF: Datos Físicos y Digitales

70 CRÍTICO

Activo:

Banco de Imágenes

Tipo:

Servicio Web

Exposición:

Base de Datos (2020)

### Ruta de cierre

1. Verificar privacidad en redes sociales.
2. Estar alerta ante correos/llamadas sospechosas.

### Impacto

- Doxing (publicación de datos privados).
- Acoso o localización física.
- Suplantación de identidad verificada.

### Descripción del evento

Filtración que incluye direcciones físicas, teléfonos y direcciones IP, combinados con datos de cuenta. Aumenta la superficie para ataques de ingeniería social.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-010

## Canva: Datos de Diseño y Geo

68 CRÍTICO

**Activo:**  
Diseño Gráfico

**Tipo:**  
SaaS

**Exposición:**  
Base de Datos (2019)

### Ruta de cierre

1. Cambiar contraseña y activar MFA.
2. Revisar actividad reciente en la cuenta.

### Impacto

- Correlación geográfica.
- Ataques de phishing temáticos (diseño/marketing).

### Descripción del evento

Exposición de datos de usuario, ubicación geográfica y hashes de contraseña.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-009

## MyFitnessPal: Datos de Perfil

65 CRÍTICO

Activo:

Salud / Lifestyle

Tipo:

Aplicación Móvil

Exposición:

Brecha Masiva (2018)

### Ruta de cierre

1. Cambiar contraseña si es compartida.
2. Desvincular integraciones con redes sociales.

### Impacto

- Perflado de usuario para marketing o estafas.
- Acceso lateral a otras cuentas.

### Descripción del evento

Exposición de correos, usuarios y contraseñas. Aunque no incluye datos financieros, permite correlacionar hábitos y rutinas del usuario.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-011

## Animoto: Datos Personales

60 CRÍTICO

Activo:

Edición de Video

Tipo:

SaaS

Exposición:

Base de Datos (2018)

### Ruta de cierre

1. Monitorear preguntas de seguridad en otros servicios.

### Impacto

- Uso de fecha de nacimiento para recuperar otras cuentas.
- Suplantación de identidad básica.

### Descripción del evento

Inclusión de fechas de nacimiento y geolocalización junto a credenciales. La fecha de nacimiento es un dato crítico para verificaciones de seguridad.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-013

## Manipulated Caiman: Blanco de Phishing

58 ALTO

Activo:

Email Personal

Tipo:

Campaña de Amenaza

Exposición:

Target List (2023)

### Ruta de cierre

1. Extrema precaución con adjuntos y enlaces.
2. Mejorar filtros de spam/seguridad en el correo.

### Impacto

- Recepción de correos maliciosos altamente personalizados.
- Riesgo de infección por malware.

### Descripción del evento

Su dirección de correo ha sido identificada en listas de objetivos de la campaña de phishing 'Manipulated Caiman', enfocada en usuarios de México.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-012

## Dropbox: Hash de Contraseñas

55 ALTO

Activo:

Almacenamiento Cloud

Tipo:

Infraestructura

Exposición:

Base de Datos (2012)

### Ruta de cierre

1. Asegurar que la contraseña fue cambiada post-2016.
2. Activar 2FA en Dropbox obligatoriamente.

### Impacto

- Intento de descifrado de hashes antiguos.
- Reutilización histórica.

### Descripción del evento

Brecha antigua pero relevante por la popularidad del servicio. Se filtraron hashes de contraseñas.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-014

## GeekedIn: Perfil Profesional

45 ALTO

Activo:

Desarrollo Profesional

Tipo:

Scraping

Exposición:

Base de Datos (2016)

### Ruta de cierre

1. Verificar legitimidad de reclutadores.

### Impacto

- Ofertas de trabajo falsas (Job Scams).
- Ingeniería social basada en perfil laboral.

### Descripción del evento

Exposición de datos profesionales: habilidades, experiencia y ubicación. Útil para reclutadores falsos o ingeniería social corporativa.



# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-015

## Twitter (200M): Identidad Social

40 ALTO

Activo:

Red Social

Tipo:

Perfil Público

Exposición:

Scraping/API (2021)

### Ruta de cierre

1. Desvincular teléfono/email de la búsqueda pública.
2. Usar alias de correo para redes sociales.

### Impacto

- Desanonimización de cuentas.
- Acoso selectivo.
- Correlación de identidad cruzada.

### Descripción del evento

Asociación del correo electrónico con el perfil de Twitter (X). Permite vincular la identidad seudónima con la real.

# Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-016

## Trello: Enumeración de Usuarios

35 MODERADO

Activo:

Gestión de Proyectos

Tipo:

SaaS

Exposición:

Scraping (2024)

### Ruta de cierre

1. Hacer tableros privados si contienen datos sensibles.
2. Ignorar correos genéricos de soporte de Trello.

### Impacto

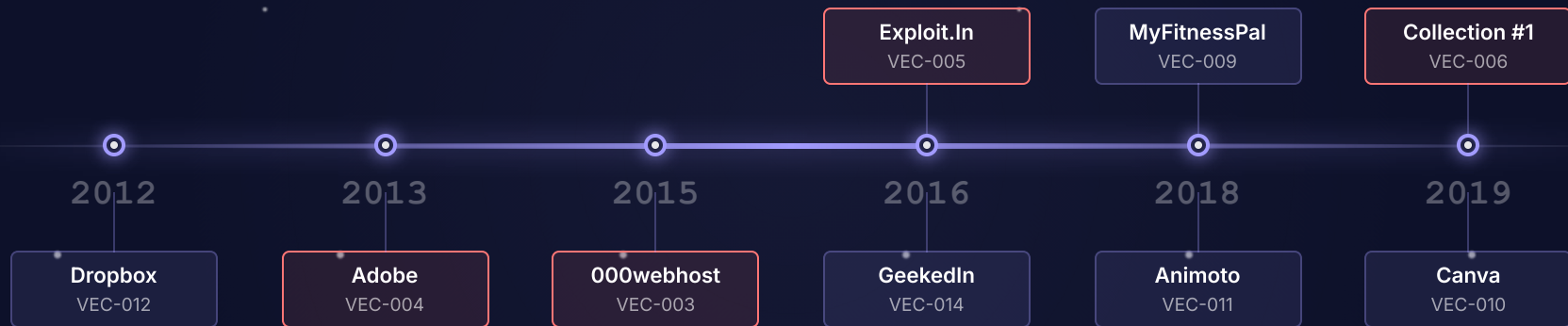
- Phishing temático de Atlassian/Trello.
- Confirmación de cuenta activa.

### Descripción del evento

Confirmación de que el correo tiene una cuenta de Trello asociada mediante enumeración de API.

# Horizonte De Exposición

Cronología de Incidentes Identificados (1/2)



# Horizonte De Exposición

Cronología de Incidentes Identificados (2/2)



# Valor De Exposición

Estimación de Impacto Financiero en Mercado Negro

CONCEPTO	CANTIDAD	PRECIO UNIT.	SUBTOTAL
Datos Financieros/Identidad Crítica	5	\$50 USD	\$250.00
Credenciales Corporativas/Personales	8	\$15 USD	\$120.00
Datos de Perfil/Huella Digital	3	\$5 USD	\$15.00
TOTAL ESTIMADO			\$385.00 USD

## Valor Total en Mercado Negro

# \$385.00 USD

**Asimetría de Riesgo:** Por una inversión trivial, el mercado negro ofrece las llaves de su organización. Este monto no refleja el valor de sus activos, sino la alarmante facilidad y bajo costo con el que un atacante puede iniciar un incidente catastrófico.

# Vector De Ataque

Cómo un atacante usaría esta información



# Impacto Directo Al Negocio

Traducción de Riesgo Técnico a Estratégico



## Financiero

Pérdida directa por fraude bancario, costos elevados de remediación y posibles multas por incumplimiento.



## Operativo

Interrupción de servicios críticos, parálisis de sistemas y pérdida de productividad empresarial.



## Reputacional

Pérdida catastrófica de confianza del cliente y daño irreversible a la imagen de marca.



## Regulatorio

Sanciones legales severas por violaciones a la LFPDPPP, GDPR y normativas de protección.

# Escenario De Inacción

La trampa de latencia: por qué no ha pasado nada no significa seguridad



Deuda histórica

## 13 años sin incidentes

Esto no es seguridad, es suerte operativa. La seguridad por oscuridad funcionaba cuando los ataques eran manuales y dirigidos.

Estado: **Obsoleto**



Nueva visibilidad

## Automatización e IA

Hoy, escáneres masivos y bots de IA encuentran vulnerabilidades en segundos. Lo que antes era invisible, ahora es un blanco automático.

Estado: **Expuesto**



Colapso inevitable

## Costo exponencial

Sistemas legados sin soporte no se pueden parchar. Una brecha hoy obliga a una reconstrucción total (10x costo) en lugar de remediación.

Estado: **Crítico**



# Ventana De Cierre

Plan de acción recomendado para la mitigación de riesgos

Fase 1

## 0-24 h

Contención inmediata

- **Cambio inteligente de credenciales**

Implementa una frase de seguridad robusta (ej. MiPerroComeCereal2024) en tu cuenta de correo principal para detener el acceso inmediato.

- **Doble candado (2FA)**

Activa la verificación en 2 pasos en WhatsApp y banca móvil. Prioriza el uso de una app autenticadora sobre los mensajes SMS.

Fase 2

## 24-72 h

Ventana táctica

- **Cierre global de sesiones**

Accede a la configuración de seguridad de Google, Facebook y bancos para forzar el cierre de sesión en todos los dispositivos no reconocidos.

- **Alertas transaccionales totales**

Configura tu banca móvil para recibir notificaciones por cargos de cualquier monto para detectar intentos de validación de tarjeta.

Fase 3

## 30 días

Estrategia a largo plazo

- **Candado crediticio (Buró)**

Solicita el servicio de bloqueo en Buró de Crédito para impedir consultas no autorizadas o apertura de créditos sin tu consentimiento.

- **Higiene digital recurrente**

Establece una rutina de revisión semanal de estados de cuenta para detectar cargos hormiga antes de un fraude mayor.

# Ruta De Cierre Consolidada

Resumen ejecutivo de acciones prioritarias por dominio



## Identidad digital

- ✓ Cambio de contraseñas del correo principal.
- ✓ Activar verificación en 2 pasos (WhatsApp/Email).
- ✓ Usar un gestor de claves seguro.
- ✓ Revisar qué apps tienen acceso a tu cuenta.
- ✓ Borrar cuentas de sitios que ya no usas.



## Seguridad financiera

- ✓ Bloqueo de consultas en Buró de Crédito.
- ✓ Activar notificaciones por cualquier gasto (\$0).
- ✓ Solicitar reposición de tarjetas expuestas.
- ✓ Bajar límites de gasto diario en la App.
- ✓ Vincular huella/rostro en la app del banco.



## Higiene & privacidad

- ✓ Cerrar sesión en todos los dispositivos.
- ✓ Ocultar ubicación y datos en redes sociales.
- ✓ Revisar estados de cuenta cada semana.
- ✓ Imprimir y guardar códigos de recuperación.
- ✓ Asegurar teléfono con PIN de 6 dígitos.

Meta de resiliencia



Nivel proyectado: 95/100

Nivel de protección estimado tras completar la ruta sugerida en este reporte.